Collier Exposed Investigative Project

Telemetry Capture – Target Access Event - CE-T03

Author: *Michael Szabó* — Cyber Forensic Expert, Collier Exposed Investigative Project
Document Type: *Technical Intelligence Note*
Prepared: 14 March 2026
Collection Method: Controlled short-URL telemetry capture following delivery of a physical letter containing a unique tracking link.

Target Respondent

Field	Detail
Case ID	**CE-T03**
Name	**Jennifer Jesse Collier**

#COLLIEREXPOSED

Field	Detail
Address	*Flat C, 94 Holland Road, London W14 8BN*
Engagement Method	Physical letter containing a unique shortened URL
Intended Outcome	Confirmation of receipt and capture of device/network telemetry upon link access

Independent Verification

Resource	Link
Archived snapshot	https://archive.ph/bnUTU

This link allows third parties to independently verify the telemetry records referenced in this document.

Access Events & Telemetry

#COLLIEREXPOSED

Timestamp (UTC)	IP Address	ISP	Device	OS	Browser	City	Country	Coordinates
29 Feb 2024 – 22:13:37	122.56.233.202	Spark New Zealand Trading Limited	iPhone	iOS 16.6	Safari 16.6	Auckland	New Zealand	-36.8542, 174.7640
29 Feb 2024 – 22:13:29	49.225.76.20	Vodafone New Zealand Limited	iPhone	iOS 16.6	Safari 16.6	Auckland	New Zealand	-36.7847, 174.7540

Total Access Events: 2

Unique Accesses: 1

Interval Between Requests: *~8 seconds*

Device Signature

#COLLIEREXPOSED

Field	Value
Device Type	**Apple iPhone**
Operating System	iOS 16.6
Browser	Safari 16.6
Location Accuracy	IP-derived
HTTP Referrer	*None recorded*
Bot Detection	Negative
User Agent	Mozilla/5.0 (iPhone; CPU iPhone OS 16_6_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/16.6 Mobile/15E148 Safari/604.1

Analytical Observations

Two access events were recorded within an *eight-second interval*, strongly indicating a **single user interaction** resulting in near-simultaneous requests.

#COLLIEREXPOSED

Both events share **identical device characteristics**, confirming a single iPhone device was responsible.

The use of *two different New Zealand network providers* is consistent with mobile routing behaviour and does not suggest multiple devices.

Geolocation data places both requests within the *Auckland metropolitan area*.

No HTTP referrer was recorded, indicating **direct access to the link**.

The telemetry supports a **high-confidence conclusion** that the tracking link was accessed by a single iPhone device located in Auckland, suggesting the recipient or an associated party engaged with the correspondence from outside the United Kingdom.

#COLLIEREXPOSED